社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2004－ＣＳＥＣ－26　(５)
2004／7／20

KASUMI Type Pseudorandom Permutationの効率的変形に関して

李　元一[†]　櫻井　幸一[†]　洪　錫憙[††]　李　相珍[††]

† 九州大学大学院システム情報科学院　〒812-8581 福岡市東区箱崎 6-10-1
†† 高麗大学校情報保護技術研究所　〒136-701 ソウル城北区安岩洞 5-1-0
E-mail: †wonil@itslab.csce.kyushu-u.ac.jp, ††sakurai@csce.kyushu-u.ac.jp, †††hsh@cist.korea.ac.kr, ††††sangjin@korea.ac.kr

A More Efficient Modification of KASUMI Type Pseudorandom Permutations

Wonil LEE[†], Kouichi SAKURAI[†], Seokhie HONG[††], and Sangjin LEE[††]

† Faculty of Information Science and Electrical Engineering, 6-10-1, Hakozaki, Higashi-ku, Fukuoka, Japan
†† Center for Information and Security Technologies(CIST), Korea University, Seoul, KOREA
E-mail: †wonil@itslab.csce.kyushu-u.ac.jp, ††sakurai@csce.kyushu-u.ac.jp, †††hsh@cist.korea.ac.kr, ††††sangjin@korea.ac.kr

Abstract We present a modification of the KASUMI type permutations and analyze the security of it using the notion of pseudorandomness. Our modification is similar to the KASUMI type permutations except the use of just two round MISTY-type permutation as the round function. Note that the values of each round functions of two round MISTY-type permutation can be computed simultaneously. So our modified permuatation can be computed more efficiently than the original KASUMI type permuation. Furthermore our results have a sligtly more good (or same) upper bound of success probablity of arbitrary attacker in the sense of (super) pseudorandomness.

Key words *KASUMI block cipher, Pseudorandomness, Provable security*

1. Introduction

Brief history Luby and Rackoff[4] introduced a theory for the security of block ciphers by using the notion of pseudorandomness. One of the purposes of the security analysis using the notion of pseudorandomness is to measure the security of the structures used in the block ciphers. Roughly speaking, the security of the structure is analyzed after the main functions (such as round functions in Feistel transformations) is replaced with a pseudorandom function or pseudorandom permutation. With this replacement, Luby and Rackoff showed that the three round DES type permutation is a pseudorandom permutation and the four round one is a super-pseudorandom permutation.[4]

KASUMI is a block cipher which has been adopted as a standard of 3GPP[1], where 3GPP is the body standardizing the next generation of mobile telephony. The overall structure of KASUMI is a Feistel permutation and each round function consists of two functions, FL function and FO function. Each FO function consists of a three round MISTY type permutation, where each round function is called an FI function. And each FI function consists of a four round MISTY type permutation. See[1],[2] for details.

Recently Iwata, Yagi, and Kurosawa[2] presented results about the pseudorandomness of KASUMI for adaptive adversarial model. They first idealize KASUMI as follows.

- Each FL function is ignored.
- Each FI function is idealized by an independant (pseudo) random permutation.

They call such an idealized KASUMI a "KASUMI type permutation," and proved that the four round and six round idealized KASUMI type permutation are pseudorandom and super-pseudorandom, respectively, for adaptive adversaries.

Motivation The results of [2] are related to the following question:

- How to provide a construction method of a (super) pseudorandom permuation with large input size using several independent pseudorandom permutations with small input size.

More specifically, their results shows that there exist

(1) a construction method of a $4n$-bit input size pseudorandom permuation using **"twelve"** independent n-bit input size pseudorandom permutations, and

(2) a construction method of a $4n$-bit input size super pseudorandom permuation using **"eighteen"** independent n-bit input size pseudorandom permutations.

The results of [2] shows that the high level structure of KASUMI block cipher can be used to get the above results.

Here, we can think a next natural question. That is, how to reduce the number of using n-bit input size pseudorandom permutations in order to obtain a $4n$-bit input size (super) pseudorandom permuation, while it preserves security of the above results.

Our contribution In this paper, we show that there exist

(1) a construction method of a $4n$-bit input size pseudorandom permuation using **"ten"** n-bit input size pseudorandom permutations, and

(2) a construction method of a $4n$-bit input size super-pseudorandom permuation using **"sixteen"** n-bit input size pseudorandom permutations.

We will first define a modification of the high level structure of KASUMI block cipher and then prove our above results with the modified structure in the adaptive adversarial model.

Our modification is similar to the KASUMI type permutation except the use of just two round MISTY-type permutation as the round function of it. Details can be shown in Section 2.2. Here note that two round MISTY-type permutation can be computed parallelly (the values of each round functions can be computed simultaneously). So our modification can be computed more efficiently than the original KASUMI type permutation. Furthermore our results have slightly more good (or same) upper bound of success probability of arbitrary attacker in the sense of (super) pseudorandomness. A summary of our results is given by Table 1. The model of attacker (and the meaning of q) will be described momentarily.

表 1 Summary of the previous results and our contributions. (# BP means the number of basic permutations and UP an upper bound of success probability.)

	Pseudorandom		Super-pseudorandom	
	# BP	UP	# BP	UP
[2]	12	$\frac{15}{2}\cdot\frac{q(q-1)}{2^n-1}$	18	$\frac{9q(q-1)}{2^n-1}$
this paper	10	$\frac{7q(q-1)}{2^n-1}$	16	$\frac{9q(q-1)}{2^n-1}$

2. Preliminaries

Our overall treatment follows the nicely laid out framework of Iwata, Yagi, and Kurosawa [2].

2.1 Notation

For a bit string $x \in \{0,1\}^{4n}$, we denote the first n bits of x by x_{LL}, the next n bits of x by x_{LR}, the third n bits of x by x_{RL}, and the last n bits of x by x_{LL}. That is, $x = (x_{LL}, x_{LR}, x_{RL}, x_{RR})$. For a set of l-bit strings $\{x^{(i)} | x^{(i)} \in \{0,1\}^l\}_{1 \leqq i \leqq q}$, we say $\{x^{(i)}\}_{1 \leqq i \leqq q}$ are distinct to mean $x^{(i)} \neq x^{(j)}$ for $1 \leqq \forall i < \forall j \leqq q$.

If S is a set, $s \xleftarrow{R} S$ denotes the process of picking an element from S uniformly at random. Denote by P_n the set of all permutations over $\{0,1\}^n$, which consists of $(2^n)!$ permutations in total. For functions f and g, $g \circ f$ denotes the function $x \mapsto g(f(x))$.

2.2 A Modification of KASUMI type permutation

In this section, we provide the definition of our modification of KASUMI type permutations. We call it "the MKASUMI type permutation".

[Definition 1] (The basic MKASUMI type permutation) Let $x \in \{0,1\}^{4n}$. For any permutations $p_1, p_2 \in P_n$, define the basic MKASUMI type permutation $\psi_{p_1,p_2} \in P_{4n}$ as

$$\psi_{p_1,p_2}(x) = y$$

where $y_{LL} = x_{RL}$, $y_{LR} = x_{RR}$, $y_{RL} = x_{RL} \oplus p_1(x_{RR}) \oplus p_2(x_{RL}) \oplus x_{LL}$, and $y_{RR} = x_{RL} \oplus p_1(x_{RR}) \oplus x_{LL}$.

[Definition 2] (The r round MKASUMI type permutation) Let $r \geqq 1$ be an integer, and $p_1, p_2, ..., p_{2r} \in P_n$ be permutations. Define the r round MKASUMI type permutation $\psi(p_1, p_2, ..., p_{2r}) \in P_{4n}$ as

$$\psi(p_1, p_2, ..., p_{2r}) = \psi_{p_{2r-1},p_{2r}} \circ \psi_{p_{2r-3},p_{2r-2}} \circ \cdots \circ \psi_{p_1,p_2}$$

See figures in Appendix for illustrations. In this paper, for $1 \leqq i \leqq q$ and $1 \leqq j \leqq 2r$, let $I_j^{(i)}$ denote the input to p_i when the input to ψ is $x^{(i)}$ and the output is $y^{(i)}$. Similarly, let $O_j^{(i)}$ denote the output of p_i when the input to ψ is $x^{(i)}$ and the output is $y^{(i)}$.

2.3 Pseudorandom and Super-pseudorandom Permutations

Our adaptive adversary A is modeled as a Turing machine that has black-box access to an oracle (or oracles). The computational power of A is unlimited, but the total number of oracle calls is limited to a the number q. After making at

most q queries to the oracle(s) adaptively, A outputs a bit. In this paper, we assume that A never asks a query if its answer is determined by a previous query-answer pair.

The pseudorandomness of a block cipher Ψ over $\{0,1\}^{4n}$ captures its computational indistinguishability from P_{4n}, where the adversary is given access to the forward direction of the permutation. In other words, it measures security of a block cipher against adaptive chosen plaintext attack.

[Definition 3] (Pseudorandomness) Let a block cipher Ψ be a family of permutations over $\{0,1\}^{4n}$. Let A be an adversary. Then A's advantage is defined by

$$Adv_{\Psi}^{prp}(A) = |Pr(\psi \xleftarrow{R} \Psi : A^{\psi} = 1) - Pr(R \xleftarrow{R} P_{4n} : A^{R} = 1)|$$

A^{ψ} indicates A with an oracle which, in response to a query x, returns $y \leftarrow \psi(x)$. A^{R} indicates A with an oracle which, in response to a query x, returns $y \leftarrow R(x)$.

The super-pseudorandomness of a block cipher Ψ over $\{0,1\}^{4n}$ captures its computational indistinguishability from P_{4n}, where the adversary is given access to both directions of the permutation. In other words, it measures security of a block cipher against adaptive chosen plaintext and chosen ciphertext attacks.

[Definition 4] (Super-pseudorandomness) Let a block cipher Ψ be a family of permutations over $\{0,1\}^{4n}$. Let A be an adversary. Then A's advantage is defined by

$Adv_{\Psi}^{spRP}(A) =$

$$|Pr(\psi \xleftarrow{R} \Psi : A^{\psi,\psi^{-1}} = 1) - Pr(R \xleftarrow{R} P_{4n} : A^{R,R^{-1}} = 1)|$$

$A^{\psi,\psi^{-1}}$ indicates A with an oracle which, in response to a query $(+,x)$, returns $y \leftarrow \psi(x)$, and in response to a query $(-,y)$, returns $x \leftarrow \psi^{-1}(y)$. $A^{R,R^{-1}}$ indicates A with an oracle which, in response to a query $(+,x)$, returns $y \leftarrow R(x)$, and in response to a query $(-,y)$, returns $x \leftarrow R^{-1}(y)$.

3. Five round MKASUMI type permutation is pseudorandom.

[Theorem 1] For $1 \leqq i \leqq 10$, let $p_i \in P_n$ be a random permutation. Let $\psi = \psi(p_1, ..., p_{10})$ be a five round Variant KASUMI. And let $R \in P_{4n}$ be a random permutation and $\Psi = \{\psi \mid \psi = \psi(p_1, ..., p_{10}), p_i \in P_n \text{ for } 1 \leqq i \leqq 10\}$.

Then for any adversary $\mathcal{A}$ that makes at most q queries in total,

$$Adv_{\Psi}^{prp}(A) \leqq \frac{7q(q-1)}{2^n - 1}.$$

Proof Let $\mathcal{O}$ be either R or ψ. The adversary A has oracle access to $\mathcal{O}$. A can make a query x and the oracle returns $y = \mathcal{O}(x)$. For the i-th query A makes to $\mathcal{O}$, define the query-answer pair $(x^{(i)}, y^{(i)}) \in \{0,1\}^{4n} \times \{0,1\}^{4n}$, where A's query was $x^{(i)}$ and the answer it got was $y^{(i)}$. Define view v of A as $v = \langle (x^{(1)}, y^{(1)}), ..., (x^{(q)}, y^{(q)}) \rangle$.

Since A is computationally unbounded, we may without loss of generality assume that A is deterministic. This implies that for every $1 \leqq i \leqq q$ the i-th query $x^{(i)}$ is fully determined by the first $i-1$ query-answer pairs, and the final output of A (0 or 1) depends only on v. Therefore, there exists a function $C_A(\cdot)$ such that $C_A(x^{(1)}, y^{(1)}, ..., x^{(i-1)}, y^{(i-1)}) = x^{(i)}$ for $1 \leqq i \leqq q$ and$C_A(v) = A$'s final output.

We say that $v = \langle (x^{(1)}, y^{(1)}), ..., (x^{(q)}, y^{(q)}) \rangle$ is a *possible* view if for every $1 \leqq i \leqq q$, $C_A(x^{(1)}, y^{(1)}, ..., x^{(i-1)}, y^{(i-1)}) = x^{(i)}$.

Let $v_{one} = \{v | C_A(v) = 1 \text{ and } v \text{ is possible}\}$. Further, we let v_{good} be a set of all possible view $v = \langle (x^{(1)}, y^{(1)}), ..., (x^{(q)}, y^{(q)}) \rangle$ which satisfies the following four conditions: (1) $C_A(v) = 1$, (2) $\{y_{RL}^{(i)}\}_{1 \leqq i \leqq q}$ are distinct, (3) $\{y_{RR}^{(i)}\}_{1 \leqq i \leqq q}$ are distinct, and (4) $\{x_{RL}^{(i)} \oplus x_{RR}^{(i)} \oplus y_{RL}^{(i)} \oplus y_{RR}^{(i)}\}_{1 \leqq i \leqq q}$ are distinct.

Evaluation of p_R We first evaluate $p_R = Pr(R \xleftarrow{R} P_{4n} : A^R = 1)$. We have $p_R = \frac{\#\{R | A^R = 1\}}{(2^{4n})!}$. For each $v \in v_{one}$, the number of R such that

$$R(x^{(i)}) = y^{(i)} \text{ for all } 1 \leqq i \leqq q \tag{1}$$

is exactly $(2^{4n} - q)!$. Therefore, we have $p_R = \sum_{v \in v_{one}} \frac{\#\{R | R \text{ satisfying (1)}\}}{(2^{4n})!} = \#v_{one} \cdot \frac{(2^{4n}-q)!}{(2^{4n})!}$.

Evaluation of p_{ψ} We evaluate $p_{\psi} = Pr(\psi \xleftarrow{R} \Psi : A^{\psi} = 1)$, where $\psi \xleftarrow{R} \Psi$ means that $p_i \xleftarrow{R} P_n$ for $1 \leqq i \leqq 10$ and then let $\psi \leftarrow \psi(p_1, ..., p_{10})$. Then we have $p_{\psi} = \frac{\#\{(p_1,...,p_{10}) | A^{\psi} = 1\}}{((2^n)!)^{10}}$.

We have the following lemmas. A proof of Lemma 1 is given in Section 4..

[Lemma 1] (Main Lemma) For any fixed possible view $v = \langle (x^{(1)}, y^{(1)}), ..., (x^{(q)}, y^{(q)}) \rangle$ such that $\{y_{RL}^{(i)}\}_{1 \leqq i \leqq q}$ are distinct, $\{y_{RR}^{(i)}\}_{1 \leqq i \leqq q}$ are distinct, and $\{x_{RL}^{(i)} \oplus x_{RR}^{(i)} \oplus y_{RL}^{(i)} \oplus y_{RR}^{(i)}\}_{1 \leqq i \leqq q}$ are distinct, the number of $(p_1, ..., p_{10})$ which satisfies

$$\psi(x^{(i)}) = y^{(i)} \text{ for } 1 \leqq \forall i \leqq q \tag{2}$$

is at least $(1 - \frac{11}{2} \cdot \frac{q(q-1)}{2^n - 1}) \cdot \{2^n!\}^6 \cdot \{(2^n - q)!\}^4$.

[Lemma 2] $\#v_{good} \geqq \#v_{one} - \frac{3}{2} \cdot \frac{q(q-1)}{2^n - 1} \cdot \frac{(2^{4n})!}{(2^{4n}-q)!}$.

Proof The proof is almost similar to the proof of [2]. So we omit it.

Then from Lemma 1 and 2, we have

$$\begin{aligned} p_{\psi} &\geqq \sum_{v \in v_{good}} \frac{\#\{(p_1, ..., p_{10}) | (p_1, ..., p_{10}) \text{ satisfying (2)}\}}{\{(2^n)!\}^{10}} \\ &\geqq \sum_{v \in v_{good}} (1 - \frac{11}{2} \cdot \frac{q(q-1)}{2^n - 1}) \cdot \frac{\{(2^n - q)!\}^4}{\{(2^n)!\}^4} \\ &\geqq (\#v_{one} - \frac{3}{2} \cdot \frac{q(q-1)}{2^n - 1} \cdot \frac{(2^{4n})!}{(2^{4n} - q)!}) \\ &\quad \cdot (1 - \frac{11}{2} \cdot \frac{q(q-1)}{2^n - 1}) \cdot \frac{\{(2^n - q)!\}^4}{\{(2^n)!\}^4} \end{aligned}$$

$$= (p_R - \frac{3}{2}\cdot\frac{q(q-1)}{2^n-1})\cdot(1-\frac{11}{2}\cdot\frac{q(q-1)}{2^n-1})$$
$$\cdot\frac{\{(2^n-q)!\}^4}{\{(2^n)!\}^4}\cdot\frac{(2^{4n})!}{(2^{4n}-q)!}$$

Now it is easy to see that $\frac{\{(2^n-q)!\}^4}{\{(2^n)!\}^4}\cdot\frac{(2^{4n})!}{(2^{4n}-q)!} \geqq 1$ (this can be shown easily by an induction on q). Then $p_\psi \geqq (p_R - \frac{3}{2}\cdot\frac{q(q-1)}{2^n-1})\cdot(1-\frac{11}{2}\cdot\frac{q(q-1)}{2^n-1}) \geqq p_R - \frac{7q(q-1)}{2^n-1}$. Applying the same argument to $1-p_\psi$ and $1-p_R$ yields that $1-p_\psi \geqq 1-p_R-\frac{7q(q-1)}{2^n-1}$, and we have $|p_\psi - p_R| \leqq \frac{7q(q-1)}{2^n-1}$.

From Theorem 1, it is very easy to show $\psi = \psi(p_1,...,p_{10})$ is pseudorandom even if each p_i is a pseudorandom permutation by using a standard hybrid argument [4].

4. Proof of Lemma 1

First, we need following two lemmas.

[Lemma 3] Let $v = \langle (x^{(1)},y^{(1)}),...,(x^{(q)},y^{(q)})\rangle$ be a fixed possible view. Then

$$\#\{(p_1,p_2,p_3,p_4)|\ \exists\, i,j \text{ such that } 1\leqq i<j\leqq q \text{ and } I_6^{(i)} = I_6^{(j)}\}$$
$$\leqq \frac{q(q-1)}{2}\cdot\frac{3\cdot\{(2^n)!\}^4}{2^n-1}.$$

Proof First we fix i and j such that $1\leqq i<j\leqq q$, and consider the condition

$$I_6^{(i)} = I_6^{(j)} \tag{3}$$

in the following *four* cases:

Case 1: $x_{RR}^{(i)} \neq x_{RR}^{(j)}$. First, consider the condition

$$p_1(x_{RR}^{(i)})\oplus x_{RL}^{(i)}\oplus x_{LL}^{(i)} = p_1(x_{RR}^{(j)})\oplus x_{RL}^{(j)}\oplus x_{LL}^{(j)}. \tag{4}$$

The number of p_1 which satisfies (4) is at most $\frac{(2^n)!}{2^n-1}$ since $x_{RR}^{(i)} \neq x_{RR}^{(j)}$. Thus

$$\#\{\ (p_1,p_2,p_3,p_4)|\ (p_1,p_2,p_3,p_4) \text{ satisfies both (3) and (4)}\}$$
$$\leqq \frac{\{(2^n)!\}^4}{2^n-1}. \tag{5}$$

Next, consider any p_1 which does not satisfy (4), that is,

$$p_1(x_{RR}^{(i)})\oplus x_{RL}^{(i)}\oplus x_{LL}^{(i)} \neq p_1(x_{RR}^{(j)})\oplus x_{RL}^{(j)}\oplus x_{LL}^{(j)}. \tag{$\neg$4}$$

For this p_1, we consider the condition

$$p_2(x_{RL}^{(i)})\oplus p_1(x_{RR}^{(i)})\oplus x_{RL}^{(i)}\oplus x_{LL}^{(i)}$$
$$= p_2(x_{RL}^{(j)})\oplus p_1(x_{RR}^{(j)})\oplus x_{RL}^{(j)}\oplus x_{LL}^{(j)} \tag{6}$$

which is equivalent to $I_4^{(i)} = I_4^{(j)}$. Since ($\neg$4) holds, the number of p_2 which satisfies (6) is at most $\frac{(2^n)!}{2^n-1}$, and thus we have

$$\#\{\ (p_1,p_2,p_3,p_4)|\ (p_1,p_2,p_3,p_4) \text{ satisfies (3), ($\neg$4), and (6)}\}$$
$$\leqq \frac{\{(2^n)!\}^4}{2^n-1}. \tag{7}$$

Next, consider any p_1 which satisfies ($\neg$4), and any p_2 which dose not satisfy (6). That is,

$$p_2(x_{RL}^{(i)})\oplus p_1(x_{RR}^{(i)})\oplus x_{RL}^{(i)}\oplus x_{LL}^{(i)}$$
$$\neq p_2(x_{RL}^{(j)})\oplus p_1(x_{RR}^{(j)})\oplus x_{RL}^{(j)}\oplus x_{LL}^{(j)}, \tag{$\neg$6}$$

which is equivalent to $I_4^{(i)} \neq I_4^{(j)}$. For these p_1,p_2, and any p_3, the number of p_4 which satisfies

$$p_4(I_4^{(i)})\oplus O_3^{(i)}\oplus I_4^{(i)}\oplus X_{RL}^{(i)}$$
$$= p_4(I_4^{(j)})\oplus O_3^{(j)}\oplus I_4^{(j)}\oplus X_{RL}^{(j)},$$

which is equivalent to (3), is at most $\frac{(2^n)!}{2^n-1}$. Thus,

$$\#\{\ (p_1,p_2,p_3,p_4)|\ (p_1,p_2,p_3,p_4) \text{ satisfies (3), ($\neg$4), and ($\neg$6)}\} \leqq \frac{\{(2^n)!\}^4}{2^n-1}. \tag{8}$$

Thus, from (5),(7), and (8), we have

$$\#\{\ (p_1,p_2,p_3,p_4)|\ (p_1,p_2,p_3,p_4) \text{ satisfies (3)}\}$$
$$\leqq \frac{3\cdot\{(2^n)!\}^4}{2^n-1}. \tag{9}$$

Case 2: $x_{RL}^{(i)} \neq x_{RL}^{(j)}$ **and** $x_{RR}^{(i)} = x_{RR}^{(j)}$. For any p_1, the number of p_2 which satisfies (6) is at most $\frac{(2^n)!}{2^n-1}$ since $x_{RL}^{(i)} \neq x_{RL}^{(j)}$, and thus we have

$$\#\{\ (p_1,p_2,p_3,p_4)|\ (p_1,p_2,p_3,p_4) \text{ satisfies (3) and (6)}\}$$
$$\leqq \frac{\{(2^n)!\}^4}{2^n-1}. \tag{10}$$

Next, for any p_1, any p_2 which satisfies ($\neg$6), and any p_3, the number of p_4 which satisfies (3) is at most $\frac{(2^n)!}{2^n-1}$. Therefore we have

$$\#\{\ (p_1,p_2,p_3,p_4)|\ (p_1,p_2,p_3,p_4) \text{ satisfies (3) and ($\neg$6)}\}$$
$$\leqq \frac{\{(2^n)!\}^4}{2^n-1}. \tag{11}$$

Thus, from (10), and (11), we have

$$\#\{\ (p_1,p_2,p_3,p_4)|\ (p_1,p_2,p_3,p_4) \text{ satisfies (3)}\}$$
$$\leqq \frac{2\cdot\{(2^n)!\}^4}{2^n-1}. \tag{12}$$

Case 3: $x_{LL}^{(i)} \neq x_{LL}^{(j)}$, $x_{RL}^{(i)} = x_{RL}^{(j)}$, **and** $x_{RR}^{(i)} = x_{RR}^{(j)}$. For any p_1 and any p_2, ($\neg$6) is satisfied. Therefore, for any p_1, any p_2, and any p_3, the number of p_4 which satisfies (3) is at most $\frac{(2^n)!}{2^n-1}$. Thus we have

$$\#\{\ (p_1,p_2,p_3,p_4)|\ (p_1,p_2,p_3,p_4) \text{ satisfies (3)}\}$$
$$\leqq \frac{\{(2^n)!\}^4}{2^n-1}. \tag{13}$$

Case 4: $x_{LR}^{(i)} \neq x_{LR}^{(j)}$, $x_{LL}^{(i)} = x_{LL}^{(j)}$, $x_{RL}^{(i)} = x_{RL}^{(j)}$, **and** $x_{RR}^{(i)} = x_{RR}^{(j)}$. In this case, there exists no p_1,p_2,p_3, and p_4 that satisfies (3). Therefore we have

$$\#\{(p_1,p_2,p_3,p_4)|\ (p_1,p_2,p_3,p_4) \text{ satisfies (3)}\} = 0. \tag{14}$$

Completing the proof. By taking the maximum of (9),(12),(13), and (14),

$$\#\{(p_1,p_2,p_3,p_4)|\ (p_1,p_2,p_3,p_4) \text{ satisfies (3)}\}$$

$\leqq \frac{4\cdot\{(2^n)!\}^4}{2^n-1}$ for any case. Finally, since we have $\binom{q}{2}$ choice of i and j, the lemma follows.

[Lemma 4] Let $v = \langle (x^{(1)},y^{(1)}),...,(x^{(q)},y^{(q)})\rangle$ be a fixed possible view. Then

$$\#\{(p_1,p_2,p_3,p_4)|\ \exists\, i,j \text{ such that } 1 \leqq i < j \leqq q \text{ and } I_5^{(i)} = I_5^{(j)}\}$$

$\leqq \frac{q(q-1)}{2}\cdot\frac{2\cdot\{(2^n)!\}^4}{2^n-1}$.

Proof If we prove the lemma in the following four cases, the proof is almost similar to the proof of Lemma 3. So we omit the details.

Case 1: $x_{RL}^{(i)} \neq x_{RL}^{(j)}$.
Case 2: $x_{RR}^{(i)} \neq x_{RR}^{(j)}$ and $x_{RL}^{(i)} = x_{RL}^{(j)}$.
Case 3: $x_{LL}^{(i)} \neq x_{LL}^{(j)}$, $x_{RL}^{(i)} = x_{RL}^{(j)}$ and $x_{RR}^{(i)} = x_{RR}^{(j)}$.
Case 4: $x_{LR}^{(i)} \neq x_{LR}^{(j)}$, $x_{LL}^{(i)} = x_{LL}^{(j)}$, $x_{RL}^{(i)} = x_{RL}^{(j)}$, and $x_{RR}^{(i)} = x_{RR}^{(j)}$.

[Lemma 5] Let $v = \langle (x^{(1)},y^{(1)}),...,(x^{(q)},y^{(q)})\rangle$ be a fixed possible view such that $\{x_{RL}^{(i)} \oplus x_{RR}^{(i)} \oplus y_{RL}^{(i)} \oplus y_{RR}^{(i)}\}_{1\leqq i\leqq q}$ are distinct. Then

$$\#\{(p_1,p_2,p_3,p_4)|\ \exists\, i,j \text{ such that } 1 \leqq i < j \leqq q \text{ and } O_8^{(i)} = O_8^{(j)}\}$$

$\leqq \frac{q(q-1)}{2}\cdot\frac{\{(2^n)!\}^4}{2^n-1}$

Proof First, we fix i and j such that $1 \leqq i < j \leqq q$, and consider the condition $O_8^{(i)} = O_8^{(j)}$. Now observe that $O_8^{(i)} = O_8^{(j)}$ is equivalent to the following condition:

$$p_4(I_4^{(i)}) \oplus x_{RL}^{(i)} \oplus y_{RL}^{(i)} \oplus x_{RR}^{(i)} \oplus y_{RR}^{(i)}$$
$$= p_4(I_4^{(j)}) \oplus x_{RL}^{(j)} \oplus y_{RL}^{(j)} \oplus x_{RR}^{(j)} \oplus y_{RR}^{(j)}.$$

Then the number of p_4 which satisfies the above condition is at most $\frac{(2^n)!}{2^n-1}$, since our assumption. Therefore,

$$\#\{(p_1,p_2,p_3,p_4)|\ (p_1,p_2,p_3,p_4) \text{ satisfies } O_8^{(i)} = O_8^{(j)}\}$$

$\leqq \frac{\{(2^n)!\}^4}{2^n-1}$ and since we have $\binom{q}{2}$ choice of i and j the lemma follows.

Proof of Lemma 1 (See figures in Appendix.) Initially, $x^{(1)},...,x^{(q)},y^{(1)},...,y^{(q)}$ are fixed.

Number of $(p_1,...,p_4)$**.** From Lemma 3, 4, and 5, the number of $(p_1,...,p_4)$ such that:

- $I_5^{(i)} \neq I_5^{(j)}$, $I_6^{(i)} \neq I_6^{(j)}$, and $O_8^{(i)} \neq O_8^{(j)}$ for $1 \leqq \forall i < \forall j \leqq q$,

is at least $\{2^n!\}^4 - \frac{q(q-1)}{2}\cdot\frac{\{2^n!\}^4}{2^n-1} - \frac{2q(q-1)}{2}\cdot\frac{\{2^n!\}^4}{2^n-1} - \frac{3q(q-1)}{2}\cdot\frac{\{2^n!\}^4}{2^n-1}$. Fix any $(p_1,...,p_4)$ which satisfy these three conditions.

Number of p_5**.** For any fixed i and j such that $1 \leqq i < j \leqq q$, the number of p_5 such that

$$p_5(I_5^{(i)}) \oplus I_6^{(i)} \oplus I_3^{(i)} = p_5(I_5^{(j)}) \oplus I_6^{(j)} \oplus I_3^{(j)},$$

which is equivalent to $I_7^{(i)} = I_7^{(j)}$, is at most $\frac{(2^n)!}{2^n-1}$, since $I_5^{(i)} \neq I_5^{(j)}$.

Similarly, the number of p_5 such that

$$p_5(I_5^{(i)})\oplus I_3^{(i)}\oplus I_6^{(i)}\oplus y_{LR}^{(i)}\oplus y_{RL}^{(i)} = p_5(I_5^{(j)})\oplus I_3^{(j)}\oplus I_6^{(j)}\oplus y_{LR}^{(j)}\oplus y_{RL}^{(j)},$$

which is equivalent to $O_9^{(i)} = O_9^{(j)}$, is at most $\frac{(2^n)!}{2^n-1}$, since $I_5^{(i)} \neq I_5^{(j)}$.

Then the number of p_5 which satisfies:

- $I_7^{(i)} \neq I_7^{(j)}$ and $O_9^{(i)} \neq O_9^{(j)}$ for $1 \leqq \forall i < \forall j \leqq q$,

is at least $(2^n)! - \frac{q(q-1)\{(2^n)!\}}{2^n-1}$. Fix any p_5 which satisfy the above two conditions.

Number of p_6**.** For any fixed i and j such that $1 \leqq i < j \leqq q$, the number of p_6 such that

$$p_6(I_6^{(i)}) \oplus I_6^{(i)} \oplus O_3^{(i)} \oplus O_5^{(i)} \oplus x_{RR}^{(i)} \oplus y_{RR}^{(i)}$$
$$= p_6(I_6^{(j)}) \oplus I_6^{(j)} \oplus O_3^{(j)} \oplus O_5^{(j)} \oplus x_{RR}^{(j)} \oplus y_{RR}^{(j)},$$

which is equivalent to $O_7^{(i)} = O_7^{(j)}$, is at most $\frac{(2^n)!}{2^n-1}$, since $I_6^{(i)} \neq I_6^{(j)}$.

Similarly, the number of p_6 satisfies

$$p_6(I_6^{(i)}) \oplus I_4^{(i)} \oplus I_6^{(i)} \oplus O_5^{(i)} = p_6(I_6^{(j)}) \oplus I_4^{(j)} \oplus I_6^{(j)} \oplus O_5^{(j)},$$

which is equivalent to $I_8^{(i)} = I_8^{(j)}$, is at most $\frac{(2^n)!}{2^n-1}$, since $I_6^{(i)} \neq I_6^{(j)}$.

Similarly, the number of p_6 satisfies

$$p_6(I_6^{(i)})\oplus I_3^{(i)}\oplus I_4^{(i)}\oplus y_{LL}^{(i)}\oplus y_{LR}^{(i)} = p_6(I_6^{(j)})\oplus I_3^{(j)}\oplus I_4^{(j)}\oplus y_{LL}^{(j)}\oplus y_{LR}^{(j)},$$

which is equivalent to $O_{10}^{(i)} = O_{10}^{(j)}$, is at most $\frac{(2^n)!}{2^n-1}$, since $I_6^{(i)} \neq I_6^{(j)}$.

Then the number of p_6 satisfies:

- $O_7^{(i)} \neq O_7^{(j)}$, $I_8^{(i)} \neq I_8^{(j)}$, and $O_{10}^{(i)} \neq O_{10}^{(j)}$ for $1 \leqq \forall i < \forall j \leqq q$,

is at least $(2^n)! - \frac{3q(q-1)\{(2^n)!\}}{2(2^n-1)}$. Fix any p_6 which satisfy the above three conditions.

Number of $(p_7,...,p_{10})$**.** Now $p_1,...,p_6$ are fixed in such a way that $\{I_7^{(i)}\}_{1\leqq i\leqq q}$ are distinct, $\{O_7^{(i)}\}_{1\leqq i\leqq q}$ are distinct, $\{I_8^{(i)}\}_{1\leqq i\leqq q}$ are distinct, $\{O_8^{(i)}\}_{1\leqq i\leqq q}$ are distinct, $\{O_9^{(i)}\}_{1\leqq i\leqq q}$ are distinct, and $\{O_{10}^{(i)}\}_{1\leqq i\leqq q}$ are distinct. We know from our condition that $\{I_9^{(i)}\}_{1\leqq i\leqq q}$ are distinct and $\{I_{10}^{(i)}\}_{1\leqq i\leqq q}$ are distinct. Therefore, we have exactly $(2^n-q)!$ choice of p_i for each $i = 7,8,9,10$.

Completing the proof To summarize, we have:

- at least $(1-3\cdot\frac{q(q-1)}{2^n-1})\cdot\{2^n!\}^4$ choice of $p_1,...,p_4$.
- at least $(1-\frac{q(q-1)}{2^n-1})\cdot\{2^n!\}$ choice of p_5.
- at least $(1-\frac{3}{2}\cdot\frac{q(q-1)}{2^n-1})\cdot\{2^n!\}$ choice of p_6.
- exactly $\{(2^n-q)!\}^4$ choice of $p_7,...,p_{10}$.

Then the number of $(p_1, ..., p_{10})$ which satisfy (2) is at least

$$(1-3\cdot\frac{q(q-1)}{2^n-1})\cdot(1-\frac{q(q-1)}{2^n-1})\cdot(1-\frac{3}{2}\cdot\frac{q(q-1)}{2^n-1})\cdot\{2^n!\}^6$$

$$\cdot\{(2^n-q)!\}^4 \geqq (1-\frac{11}{2}\cdot\frac{q(q-1)}{2^n-1})\cdot\{2^n!\}^6\cdot\{(2^n-q)!\}^4.$$

5. Eight Round MKASUMI type permutation is super-pseudorandom.

[Theorem 2] For $1 \leqq i \leqq 16$, let $p_i \in P_n$ be a random permutation. Let $\psi = \psi(p_1, ..., p_{16})$ be the eight round Variant KASUMI. And let $R \in P_{4n}$ be a random permutation and $\Psi = \{\psi \mid \psi = \psi(p_1, ..., p_{16}), p_i \in P_n \text{ for } 1 \leqq i \leqq 16\}$.

Then for any adversary $\mathcal{A}$ that makes at most q queries in total,

$$Adv_{\Psi}^{sprp}(A) \leqq \frac{9q(q-1)}{2^n-1}.$$

Proof Let $\mathcal{O}$ be either R or ψ. The adversary A has oracle access to $\mathcal{O}$ and $\mathcal{O}^{-1}$. There are two types of queries A can make: either $(+,x)$ or $(-,y)$. For the i-th query A makes to $\mathcal{O}$ or $\mathcal{O}^{-1}$, define the query-answer pair $(x^{(i)}, y^{(i)}) \in \{0,1\}^{4n}\times\{0,1\}^{4n}$, where either A's query was $(+,x)$ and the answer it got was $y^{(i)} = \mathcal{O}(x^{(i)})$ or A's query was $(-,y)$ and the answer it got was $x^{(i)} = \mathcal{O}^{-1}(y^{(i)})$. Define view v of A as $v = \langle(x^{(1)}, y^{(1)}), ..., (x^{(q)}, y^{(q)})\rangle$.

Since A is computationally unbounded, we may without loss of generality assume that A is deterministic. This implies that for every $1 \leqq i \leqq q$ the i-th query $x^{(i)}$ is fully determined by the first $i-1$ query-answer pairs, and the final output of A (0 or 1) depends only on v. Therefore, there exists a function $C_A(\cdot)$ such that $C_A(x^{(1)}, y^{(1)}, ..., x^{(i-1)}, y^{(i-1)}) =$ either $(+, x^{(i)})$ or $(-, y^{(i)})$ for $1 \leqq i \leqq q$ and $C_A(v) =$ A's final output.

We say that $v = \langle(x^{(1)}, y^{(1)}), ..., (x^{(q)}, y^{(q)})\rangle$ is a *possible* view if for every $1 \leqq i \leqq q$, $C_A(x^{(1)}, y^{(1)}, ..., x^{(i-1)}, y^{(i-1)}) \in \{(+, x^{(i)}), (-, y^{(i)})\}$. Let $v_{one} = \{v | C_A(v) = 1 \text{ and } v \text{ is possible}\}$.

Evaluation of p_R We first evaluate $p_R = Pr(R \xleftarrow{R} P_{4n} : A^{R,R^{-1}} = 1)$. We have $p_R = \#v_{one}\cdot\frac{(2^{4n}-q)!}{(2^{4n})!}$ as was done in the proof of Theorem 1.

Evaluation of p_ψ We evaluate $p_\psi = Pr(\psi \xleftarrow{R} \Psi : A^{\psi,\psi^{-1}} = 1)$, where $\psi \xleftarrow{R} \Psi$ means that $p_i \xleftarrow{R} P_n$ for $1 \leqq i \leqq 16$ and then let $\psi \leftarrow \psi(p_1, ..., p_{16})$. Then we have $p_\psi = \frac{\#\{(p_1,...,p_{16}) | A^{\psi,\psi^{-1}}=1\}}{((2^n)!)^{16}}$.

We have the following main lemma. A proof of this lemma is given in Section 6..

[Lemma 6] (Main Lemma) For any fixed possible view $v = \langle(x^{(1)}, y^{(1)}), ..., (x^{(q)}, y^{(q)})\rangle$, the number of $(p_1, ..., p_{16})$ which satisfies

$$\psi(x^{(i)}) = y^{(i)} \text{ for } 1 \leqq \forall i \leqq q \qquad (15)$$

is at least $(1-\frac{9q(q-1)}{2^n-1})\cdot\{2^n!\}^{12}\cdot\{(2^n-q)!\}^4$.

Then from Lemma 6 , we have

$$\begin{aligned} p_\psi &= \sum_{v\in v_{one}} \frac{\#\{(p_1,...,p_{10})|(p_1,...,p_{16}) \text{ satisfying (15)}\}}{\{(2^n)!\}^{16}} \\ &\geqq \sum_{v\in v_{good}} (1-\frac{9q(q-1)}{2^n-1})\cdot\frac{\{(2^n-q)!\}^4}{\{(2^n)!\}^4} \\ &= \#v_{one}\cdot(1-\frac{9q(q-1)}{2^n-1})\cdot\frac{\{(2^n-q)!\}^4}{\{(2^n)!\}^4} \\ &= p_R\cdot(1-\frac{9q(q-1)}{2^n-1})\cdot\frac{\{(2^n-q)!\}^4}{\{(2^n)!\}^4}\cdot\frac{(2^{4n})!}{(2^{4n}-q)!}. \end{aligned}$$

Since $\frac{\{(2^n-q)!\}^4}{\{(2^n)!\}^4}\cdot\frac{(2^{4n})!}{(2^{4n}-q)!} \geqq 1$, $p_\psi \geqq p_R\cdot(1-\frac{9q(q-1)}{2^n-1}) \geqq p_R - \frac{9q(q-1)}{2^n-1}$. Applying the same argument to $1-p_\psi$ and $1-p_R$ yields that $1-p_\psi \geqq 1-p_R-\frac{9q(q-1)}{2^n-1}$ and we have $|p_\psi - p_R| \leqq \frac{9q(q-1)}{2^n-1}$.

6. Proof of Lemma 6

Initially, $x^{(1)}, ..., x^{(q)}, y^{(1)}, ..., y^{(q)}$ are fixed.

Number of $(p_1, ..., p_4)$. From Lemma 3 and 4, the number of $(p_1, ..., p_4)$ such that $I_5^{(i)} \neq I_5^{(j)}$ and $I_6^{(i)} \neq I_6^{(j)}$ for $1 \leqq \forall i < \forall j \leqq q$, is at least $\{2^n!\}^4 - \frac{2q(q-1)}{2}\cdot\frac{\{2^n!\}^4}{2^n-1} - \frac{3q(q-1)}{2}\cdot\frac{\{2^n!\}^4}{2^n-1}$. Fix any $(p_1, ..., p_4)$ which satisfy the above two conditions.

Number of $(p_{13}, ..., p_{16})$. From Lemma 3 and 4, the number of $(p_{13}, ..., p_{16})$ such that $I_{11}^{(i)} \neq I_{11}^{(j)}$ and $I_{12}^{(i)} \neq I_{12}^{(j)}$ for $1 \leqq \forall i < \forall j \leqq q$, is at least $\{2^n!\}^4 - \frac{2q(q-1)}{2}\cdot\frac{\{2^n!\}^4}{2^n-1} - \frac{3q(q-1)}{2}\cdot\frac{\{2^n!\}^4}{2^n-1}$. We have used the symmetry of MKASUMI type permutation. Fix any $(p_{13}, ..., p_{16})$ which satisfy the above two conditions.

Number of p_5. For any fixed i and j such that $1 \leqq i < j \leqq q$, the number of p_5 such that

$$p_5(I_5^{(i)}) \oplus I_6^{(i)} \oplus I_3^{(i)} = p_5(I_5^{(j)}) \oplus I_6^{(j)} \oplus I_3^{(j)},$$

which is equivalent to $I_7^{(i)} = I_7^{(j)}$, is at most $\frac{(2^n)!}{2^n-1}$, since $I_5^{(i)} \neq I_5^{(j)}$.

Then the number of p_5 which satisfies $I_7^{(i)} \neq I_7^{(j)}$ for $1 \leqq \forall i < \forall j \leqq q$, is at least $(2^n)! - \frac{q(q-1)}{2}\cdot\frac{(2^n)!}{2^n-1}$. Fix any p_5 which satisfy the above condition.

Number of p_{11}. For any fixed i and j such that $1 \leqq i < j \leqq q$, the number of p_{11} such that

$$p_{11}(I_{11}^{(i)}) \oplus I_{12}^{(i)} \oplus I_{13}^{(i)} = p_{11}(I_{11}^{(j)}) \oplus I_{12}^{(j)} \oplus I_{13}^{(j)},$$

which is equivalent to $I_9^{(i)} = I_9^{(j)}$, is at most $\frac{(2^n)!}{2^n-1}$, since $I_{11}^{(i)} \neq I_{11}^{(j)}$.

Then the number of p_{11} which satisfies $I_9^{(i)} \neq I_9^{(j)}$ for $1 \leqq \forall i < \forall j \leqq q$, is at least $(2^n)! - \frac{q(q-1)}{2}\cdot\frac{(2^n)!}{2^n-1}$. Fix any p_{11} which satisfy the above condition.

Number of p_6. For any fixed i and j such that $1 \leqq i < j \leqq q$, the number of p_6 such that

$$p_6(I_6^{(i)}) \oplus I_6^{(i)} \oplus O_3^{(i)} \oplus O_5^{(i)} \oplus x_{RR}^{(i)} \oplus I_9^{(i)}$$

$$= p_6(I_6^{(j)}) \oplus I_6^{(j)} \oplus O_3^{(j)} \oplus O_5^{(j)} \oplus x_{RR}^{(j)} \oplus I_9^{(j)},$$

which is equivalent to $O_7^{(i)} = O_7^{(j)}$, is at most $\frac{(2^n)!}{2^n-1}$, since $I_6^{(i)} \neq I_6^{(j)}$.

Similarly, the number of p_6 satisfies

$$p_6(I_6^{(i)}) \oplus I_4^{(i)} \oplus I_6^{(i)} \oplus O_5^{(i)} = p_6(I_6^{(j)}) \oplus I_4^{(j)} \oplus I_6^{(j)} \oplus O_5^{(j)},$$

which is equivalent to $I_8^{(i)} = I_8^{(j)}$, is at most $\frac{(2^n)!}{2^n-1}$, since $I_6^{(i)} \neq I_6^{(j)}$.

Similarly, the number of p_6 satisfies

$$p_6(I_6^{(i)}) \oplus I_3^{(i)} \oplus I_4^{(i)} \oplus I_{11}^{(i)} \oplus I_{12}^{(i)} = p_6(I_6^{(j)}) \oplus I_3^{(j)} \oplus I_4^{(j)} \oplus I_{11}^{(j)} \oplus I_{12}^{(j)},$$

which is equivalent to $O_{10}^{(i)} = O_{10}^{(j)}$, is at most $\frac{(2^n)!}{2^n-1}$, since $I_6^{(i)} \neq I_6^{(j)}$.

Then the number of p_6 satisfies $O_7^{(i)} \neq O_7^{(j)}$, $I_8^{(i)} \neq I_8^{(j)}$, and $O_{10}^{(i)} \neq O_{10}^{(j)}$ for $1 \leqq \forall i < \forall j \leqq q$, is at least $(2^n)! - \frac{3q(q-1)}{2} \cdot \frac{(2^n)!}{2^n-1}$. Fix any p_6 which satisfy the above three conditions.

Number of p_{12}. For any fixed i and j such that $1 \leqq i < j \leqq q$, the number of p_{12} such that

$$p_{12}(I_{12}^{(i)}) \oplus I_7^{(i)} \oplus I_{12}^{(i)} \oplus O_{11}^{(i)} \oplus O_{13}^{(i)} \oplus y_{LR}^{(i)}$$

$$= p_{12}(I_{12}^{(j)}) \oplus I_7^{(j)} \oplus I_{12}^{(j)} \oplus O_{11}^{(j)} \oplus O_{13}^{(j)} \oplus y_{LR}^{(j)},$$

which is equivalent to $O_9^{(i)} = O_9^{(j)}$, is at most $\frac{(2^n)!}{2^n-1}$, since $I_{12}^{(i)} \neq I_{12}^{(j)}$.

Similarly, the number of p_{12} satisfies

$$p_{12}(I_{12}^{(i)}) \oplus I_{12}^{(i)} \oplus I_{14}^{(i)} \oplus O_{11}^{(i)} = p_{12}(I_{12}^{(j)}) \oplus I_{12}^{(j)} \oplus I_{14}^{(j)} \oplus O_{11}^{(j)},$$

which is equivalent to $I_{10}^{(i)} = I_{10}^{(j)}$, is at most $\frac{(2^n)!}{2^n-1}$, since $I_{12}^{(i)} \neq I_{12}^{(j)}$.

Similarly, the number of p_{12} satisfies

$$p_{12}(I_{12}^{(i)}) \oplus I_5^{(i)} \oplus I_6^{(i)} \oplus I_{13}^{(i)} \oplus I_{14}^{(i)} = p_{12}(I_{12}^{(j)}) \oplus I_5^{(j)} \oplus I_6^{(j)} \oplus I_{13}^{(j)} \oplus I_{14}^{(j)},$$

which is equivalent to $O_8^{(i)} = O_8^{(j)}$, is at most $\frac{(2^n)!}{2^n-1}$, since $I_{12}^{(i)} \neq I_{12}^{(j)}$.

Then the number of p_{12} satisfies $O_9^{(i)} \neq O_9^{(j)}$, $I_{10}^{(i)} \neq I_{10}^{(j)}$, and $O_8^{(i)} \neq O_8^{(j)}$ for $1 \leqq \forall i < \forall j \leqq q$, is at least $(2^n)! - \frac{3q(q-1)}{2} \cdot \frac{(2^n)!}{2^n-1}$. Fix any p_{12} which satisfy the above three conditions.

Number of $(p_7, ..., p_{10})$. Now $p_1, ..., p_6, p_{11}, ..., p_{16}$ are fixed in such a way that $\{I_7^{(i)}\}_{1 \leqq i \leqq q}$ are distinct, $\{O_7^{(i)}\}_{1 \leqq i \leqq q}$ are distinct, $\{I_8^{(i)}\}_{1 \leqq i \leqq q}$ are distinct, $\{O_8^{(i)}\}_{1 \leqq i \leqq q}$ are distinct, $\{I_9^{(i)}\}_{1 \leqq i \leqq q}$ are distinct, $\{O_9^{(i)}\}_{1 \leqq i \leqq q}$ are distinct, $\{I_{10}^{(i)}\}_{1 \leqq i \leqq q}$ are distinct, and $\{O_{10}^{(i)}\}_{1 \leqq i \leqq q}$ are distinct.

Therefore, we have exactly $(2^n - q)!$ choice of p_i for each $i = 7, 8, 9, 10$.

Completing the proof To summarize, we have:

- at least $(1 - \frac{5}{2} \cdot \frac{q(q-1)}{2^n-1})^2 \cdot \{2^n!\}^8$ choice of $p_1, ..., p_4, p_{13}, ..., p_{16}$.
- at least $(1 - \frac{1}{2} \cdot \frac{q(q-1)}{2^n-1})^2 \cdot \{2^n!\}^2$ choice of (p_5, p_{11}).
- at least $(1 - \frac{3}{2} \cdot \frac{q(q-1)}{2^n-1})^2 \cdot \{2^n!\}^2$ choice of (p_6, p_{12}).
- exactly $\{(2^n - q)!\}^4$ choice of $p_7, ..., p_{10}$.

Then the number of $(p_1, ..., p_{16})$ which satisfy (15) is at least

$$(1 - \frac{5}{2} \cdot \frac{q(q-1)}{2^n-1})^2 \cdot (1 - \frac{1}{2} \cdot \frac{q(q-1)}{2^n-1})^2 \cdot (1 - \frac{3}{2} \cdot \frac{q(q-1)}{2^n-1})^2$$

$$\cdot \{2^n!\}^{12} \cdot \{(2^n - q)!\}^4 \geqq (1 - \frac{9q(q-1)}{2^n-1}) \cdot \{2^n!\}^{12} \cdot \{(2^n - q)!\}^4.$$

7. Discussion and Concluding Remarks

In this paper, we showed that 5 round MKASUMI type permutation is pseudorandom and 8 round MKASUMI type permutation is super-pseudorandom. Until now, we found a distinguisher for 3 round MKASUMI type permutation in the notion of pseudorandomness and found a distinguisher for 4 round MKASUMI type permutation in the notion of super pseudorandomness. It is easy to make a distinguisher for 3 round MKASUMI type permutation in the notion of pseudorandomness. So we omit it. We can distinguish 4 round MKASUMI type permutation from random permutation (in the notion of super pseudorandomness) using just two plaintext queries and one ciphertext query as follows: Choose two distinct plaintexts $x^{(1)} = (a, b, c, d)$ and $x^{(2)} = (a', b, c, d)$ and denote the corresponding two ciphertexts by $y^{(1)} = (e, f, g, h)$ and $y^{(2)} = (e', f', g', h')$, respectively. Then it is easy to see that

(1) $O_3^{(1)} \oplus I_4^{(1)} \oplus O_3^{(2)} \oplus I_4^{(2)} = a \oplus a'$,
(2) $O_3^{(1)} \oplus I_4^{(1)} \oplus d = p_7(f) \oplus e \oplus h$,
(3) $O_3^{(2)} \oplus I_4^{(2)} \oplus d = p_7(f') \oplus e' \oplus h'$

By (1), (2), and (3), $p_7(f) \oplus p_7(f') = a \oplus a' \oplus e \oplus e' \oplus h \oplus h'$. Hence we can obtain the value of $p_7(f) \oplus p_7(f')$ since we know a, a', e, e', h, and h'. Next, choose ciphertext $y^{(3)} = (e, f', g \oplus p_7(f) \oplus p_7(f'), h \oplus p_7(f) \oplus p_7(f'))$ and denote the corresponding plaintext by $x^{(3)} = (a'', b'', c'', d'')$. Then it is easy to check that $c \oplus c'' = d \oplus d''$ holds. Therefore we can make a distinguisher with this property. But the following problems still remain to be solved.

- Can 4 round MKASUMI type permutation be pseudorandom?
- Can 5, 6, and 7 round MKASUMI type permutation be super-pseudorandom?

In addition, it is still open whether 5 round original KASUMI type permutation can be super-pseudorandom.

Acknowledgement : The first author was supported by the 21st Century COE program ' Reconstruction of Social Infrastructure Related to Information Science and Electrical Engineering ' of the Graduate School of Information Science and Electrical Engineering, Kyushu University.

文　献

[1] 3GPP TS 35.202 v 3.1.1. Specification of the 3GPP confidentiality and integrity algorithms, Document 2: KASUMI specification. Available at http://www.3gpp.org/tb/other/algorithms.htm.

[2] T. Iwata, T. Yagi, and K. Kurosawa. *On the Pseudorandomness of KASUMI Type Permutations*, The Eighth Australasian Conference on Information Security and Privacy, ACISP 2003, LNCS, Vol. 2727, pp. 130-141, Springer-Verlag, 2003.

[3] J. S. Kang, S. U. Shin, D. Hong, and O. Yi, *Provable security of KASUMI and 3GPP encryption mode f8*, Advances in Cryptology - ASIACRYPT 2001, LNCS 2248, pp. 255-271, Springer-Verlag, 2001.

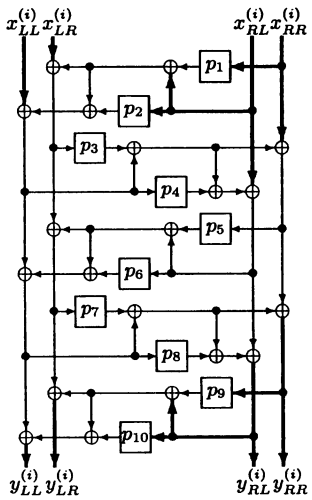
[4] M. Luby and C. Rackoff, *How to construct pseudorandom permutations from pseudoradom functions*, SIAM J. Comput., Vol. 17, no. 2, pp. 373-386, April 1988.

[5] M. Matsui, *New block encryption algorithm MISTY*, Fast Software Encryption, FSE'97, LNCS 1267, pp. 54-68, Springer-Verlag. 1997.

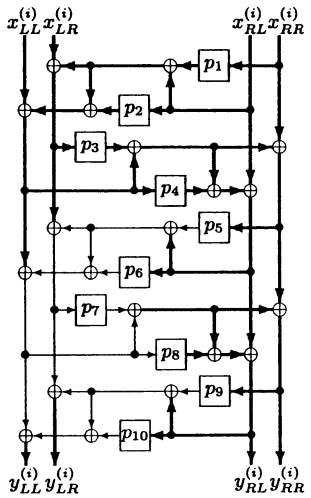
[6] J. Patarin, *Pseudorandom permutations based on the DES scheme*, Proceedings of EUROCODE'90, LNCS 514, pp. 193-204, Springer-Verlag, 1990.

[7] M. Naor and O. Reingold, *On the construction of pseudorandom permutations: Luby-Rackoff revised*, J. Cryptology, vol. 12, no. 1, pp. 29-66, Springer-Verlag, 1999.

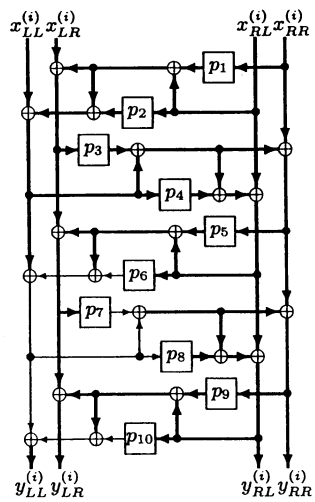
Appendix



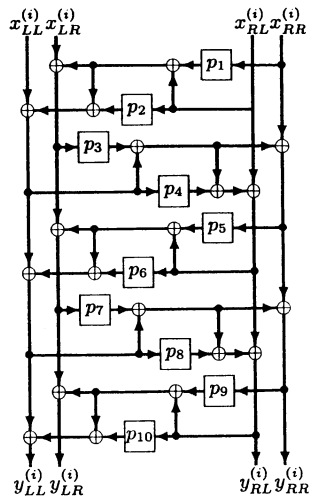
(1) $x^{(i)}$ and $y^{(i)}$ are fixed.



(2) $p_1, ..., p_4$ are fixed.



(3) p_5 is fixed.



(4) p_6 is fixed.